

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

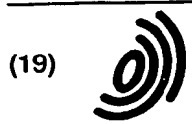
Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problems Mailbox.**



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11) EP 0 944 004 A1

(12)

EUROPEAN PATENT APPLICATION

(43) Date of publication:
22.09.1999 Bulletin 1999/38

(51) Int. Cl.⁶: G06F 17/00, H04L 29/12

(21) Application number: 98104934.9

(22) Date of filing: 18.03.1998

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC
NL PT
Designated Extension States:
AL LT LV MK RO SI

(72) Inventors:
• Bunney, William
50829 Köln (DE)
• Knox, Steve,
c/o Driftwood Systems Inc.
Lynwood, WA 98037 (US)

(71) Applicants:
• SONY EUROPE GmbH
50829 Köln (DE)
• Sony International (Europe) GmbH
50829 Köln (DE)

(74) Representative:
Rupp, Christian, Dipl.Phys. et al
Mitscherlich & Partner
Patent- und Rechtsanwälte
Sonnenstrasse 33
80331 München (DE)

(54) IRC name translation protocol

(57) A network comprising at least one server (1) and a plurality of user terminals (3), wherein the user terminals (3) can communicate with each other by means of an IRC server (40). The user terminal (3) can send a command to a chat proxy (39). The chat proxy (39) is connected with a session manager (23) to translate any address longer than nine characters (limit of the IRC protocol) to a code with a maximum length of nine characters. The chat proxy (39) can cache the result of

the conversion in a storage device (42). The chat proxy (39) then sends (41) an IRC command to the IRC server (40) together with a code having a maximum number of nine characters. The chat proxy (39) according to the present invention therefore allows a translation process, the provision of semi-private chat rooms with an additional access control and a supply of supplemental chat room attributes

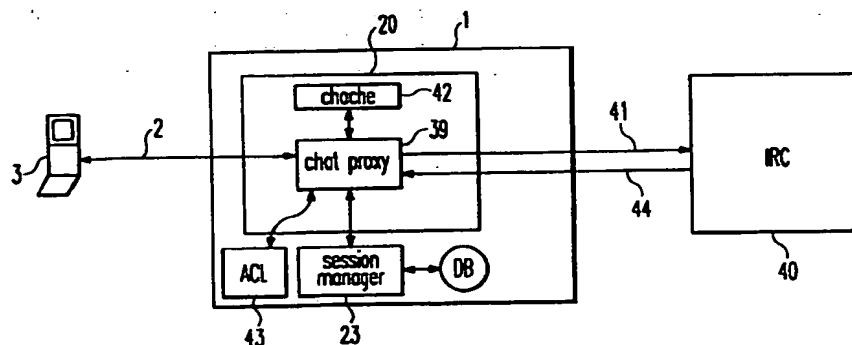


Fig. 5

shown in Fig. 1,

Fig. 3 shows a table installed in the server and containing assignment information of different addresses of one user,

Fig. 4 shows an example of the information stored in a group data base,

Fig. 5 shows in detail a structure according to an embodiment of the present invention, and

Fig. 6 shows a procedure executed according to an embodiment of the present invention.

[0016] The present invention relates to the technical field of networks particularly for an Internet application. Such a network generally should offer the following services:

- actionable messaging between individuals, or for notification of events or special offers, with the control center prompting for user response;
- web-based e-mail;
- one-to-one and many-to-many chat groups;
- discussion groups (Internet news groups)
- public event scheduling;
- online searching for people, events, and information, with results filtered based on member focus and preferences;
- a free home page
- simple tools to create and modify web pages;
- contact list management and facilities to make it easy to recruit friends and family,
- an address book and personal data base, common across a plurality of devices and services;
- the opportunity to use a plurality of identities per person, along with associated preferences and interests for each identity;
- community center;
- simple tools to enable individual members to set up and manage chat rooms and discussion groups with friends or other like-minded people;
- and innovative navigation

[0017] Further services can comprise narrowly targeted advertising, electronic commerce, and cross-platform support for intelligent devices such as telephones, televisions, or personal digital assistants.

[0018] Members of the network can have profiles of information about them, not just names and addresses, but also their interests and preferences. Members will be able to enter and edit preferences if they wish, but they need not to fill out a form to derive this benefit. Member profiles can be built up over time as a process in the system watches what they access, sign up for, or otherwise evince interest in.

[0019] User profiles can be used to filter searches, so that the results of a keyword search can be ranked according to preferences suggested by the user profile.

[0020] According to the present invention, members are able to assume several identities: for example, a personal, professional, and one identity used for fantasy or play. Members can have a home page and a profile for each identity, and can maintain anonymity in any interaction, if they so choose. Therefore a plurality of home pages respectively for one identity of a user can be assigned to one user. This will be explained in detail further below.

[0021] Users can create their home pages by answering a series of questions, and various templates can be available to make it easy for members to create their home pages and other places quickly, without learning HTML ("Places" are more than simply static text and graphics in an HTML page. They can use data from various databases, accessed by client or server applications). Generally, according to the present invention an object-oriented approach is preferred for example by using the programming language Java in combination with object-oriented data bases.

[0022] Users can control how much screen real estate to devote to the service provided by the present invention at any given moment. Depending on their degree of engagement with the system, the service can appear to members as an icon, a gadget, or a browser. If members are logged on but primarily interested in doing other work, the service will retire to a corner of the desktop as a modest icon indicating that they are logged in. In this mode, members may still receive notifications, if they choose. An intermediate degree of engagement presents the service as a "gadget" - a control center occupying minimal space on the desktop and allowing users to focus elsewhere while still maintaining immediate access to most functions. When users wish to immerse themselves in the system, they can open their favorite browser and other communication tools and integrate them with the service.

[0023] True to the central tenet of user control, the service offers members the ability to log onto the system and put

by isolating the process servers 8, 9 on a network having an IP address of the form 10.x.x.x. Routers 12 cannot connect directly to such a network. Instead, the network 2 is connected to a hub 15 connected to a bridge 14 which in turn connects to another hub 13. The hub 15 is on a network 2 to which routers 12 can connect.

[0039] The security bridge 14 protects the back-end process servers 8, 9 and databases 10, 11. A firewall could be placed between the hub 13 and the switch 14 to provide additional security for the back-end process servers 8, 9 and databases 10, 11 as well.

Clients and Front-end Processors

[0040] A user connects to the system using the control center (17 in Fig. 2) - the user's client process 3. The client process 3 connects from the Internet 2, through the router 12, to the external hub 15 and from there to a front-end processor 16: a computer 16 outside the security wall. The front-end processor 16 handles communication between the back-end server 8, 9 and the client 3 during authentication; a necessary step before the client process 3 can access.

[0041] The front-end processors 16 run so called *daemons* - background processes - for HTTP (Web access), NNTP 19 (news and discussion groups), IRC 20 (chat), and e-mail 21. They also run DNS (Domain Name Service) 22. Each front-end processor 16 may run all the required daemons. Alternatively the required daemons may be spread across several front-end processors 16.

[0042] After a user is authenticated following well known procedures, the front-end processors 16 connect the Connection Manager process to the Session Manager 23 through the bridge 14 to a process server 8, 9 and a database 10, 11.

[0043] The central installation also includes a terminal server 24 directly connected to every piece of hardware: computers, bridge 14 and router 12. An ISDN line connects this terminal server 24 to a remote location 25 where the operations manager can run tests, upgrade software, install patches, or reboot systems as necessary. The operation manager's dialup access is also secure; simply knowing the correct telephone number is not enough to gain access to the system through the maintenance channel 26.

[0044] The processes of the hardware structure shown in Fig. 1 will now be explained with reference to Fig. 2.

[0045] The software constituting the processes can be written in Java using an object-oriented design. Most of the software runs on the process servers 8, 9, but also some software is written for the front-end processor 16.

Front-end Processors

[0046] When a client process 3 (the user's control center 17) connects to a front-end processor 16, that processor's HTTP daemon 18 spawns a new thread to manage the connection as it is known in object-oriented programming. These connection managers are terminated when the user severs the connection.

[0047] The IRC and NNTP daemons 19, 20 also include specialized processes to augment their capabilities: To allow for private chats and discussion groups, both daemons include security software that allows for access control. The IRC daemon 20 also transparently translates user names required by IRC (which have a nine-character limit).

Process Servers

[0048] The bulk of the processes runs on the back-end process servers 8, 9. In addition to DNS, the processes summarized in Table 1 collaborate to provide NCP's functionality. Each is discussed in greater detail below.

Table 1

NCP Processes		
Process	Purpose	Associated database?
Session Manager 23	Tracks who is logged in (user and personality), and their current state: available, away, busy, or invisible.	session data base 50
Name Resolution 6	Correctly identifies user based on multiple identity, e.g. helps to route user notifications to the correct process server	Yes

form notifications and e-mail), and is responsible for telling the requesting service which physical system the user is logged into, thus allowing the message to be routed to the correct server. It is the sole process with access to this information, thus helping to ensure user anonymity - users will not even be able to look at mail headers and tell which city someone lives in (or near).

5

Directory services and event scheduling

[0053] This process 27, 28 can access a database 34 including all the searchable items, such as members, clubs, events, chat rooms, public or semi-private discussion groups, and home pages and other web sites. Searching is text-based; at least initially, using word-matching. Directory services 27 collaborates with the Profile Manager 4 to rank the results for relevance, based on the user's stated interests.

10

[0054] In addition, users can search for items belonging only to a particular category: for example, only discussion groups or only home pages or only people.

[0055] Event scheduling allows community organizers 35 to schedule events such as simulcasts, chats with public figures, or video conferences or other multimedia events at the most auspicious time. They can query the schedule to determine when possibly competing events are scheduled, and choose a time likely to be favorable.

15

Profile manager

[0056] Each user 3 has at least one profile, which stores not only such commonplace information as name, address, nationality and preferred language, but also a variety of more sensitive information such as age, sex, marital status, income, occupation, education, religious preference, social class, lifestyle, and other demographic and psychographic data useful for marketing purposes.

20

[0057] It is imperative that adequate safeguards ensure that:

25

- personal information is kept strictly confidential, and
- data gathered for marketing purposes is kept strictly anonymous.

[0058] This is the primary reason for the physical and hardware security described above. No aspect of the software must be allowed to compromise this security.

30

[0059] Profiles can be used for a variety of purposes:

35

- special event planning,
- FYI data gathering,
- targeted advertising
- targeted promotions and loyalty programs

[0060] When planning special events, community organizers 35 can find out how many members might be interested in the event, and can send e-mail and notifications only to those whose profiles indicate such potential interest. Although the community organizers 35 will have no knowledge of which specific individuals received their mail or notices, they will be assured that a certain number were sent, and that those who received them are more likely than most to have appreciated them.

40

[0061] The FYI process 30 uses member profiles to determine which data to gather on each member's behalf.

45 Notification server

[0062] The notification server 29 is responsible for sending *notifications* - instant messages - between individuals, and between community organizers and individuals. To do so, the notification server 29 collaborates with the session manager 23 to determine who is currently online and available, and to get a handle to the recipient's connection manager in order to deliver the message. It then communicates with the notification server 29 on the recipient's server machine, if different, to deliver the notification.

50

[0063] Notifications are of two kinds: *real-time* and *queued*. *Real-time notifications* are typically from one individual member to another. When received, they are stored on the client's machine 3. If the intended recipient is off-line or invisible, they are not delivered.

55

[0064] *Queued notifications* are sent by community organizers 35, typically to many members whom the community organizer believes will be interested. When they are created, the community organizer specifies a "time to live" - a period of time during which the notification remains relevant. If the intended recipient is off-line, they are queued in the notification server's 33 associated database 36 and delivered as soon as the recipient logs in, assuming that this occurs

invention a wrapper or proxy is provided between a chat client and the IRC server allowing the use of usual off-the-shelf IRC server software and at the same time to enhance the basic server used for the chat communications with additional features:

- 5 • name translation from any address containing more than nine characters to nicknames with nine characters compatible with IRC, and translating back to identities with addresses of more than nine characters,
- the ability to supply the IRC channel with supplemental access control lists for members (read-write-participants) and non-members (read-only-participants) which represent the same semi-private chat room,
- 10 • the ability to supply the IRC client with supplemental descriptive information about the chat channel such as for example
- community organizers (sponsors),
- organizers/operators,
- moderators, and
- a descriptive paragraph about the chat (IRC supports only the name and channel)

15 [0079] The translation and additional information transmission procedure according to the present invention will now be explained with reference to Fig. 5. A chat client can send a command to the chat proxy 39, which represents a conversion means, together with the address of the sender (terminal 3 e.g.). The chat proxy 39 contacts the session manager 23 to get a unique nickname with nine characters for the user 3. The session manager 23 accesses the session data base 50. This nickname supplied from the session manager 23 to the chat proxy 39 is required to be unique only
20 with the current on-line users, it does not need to be unique across time and space. Therefore, a nick can be reused after the user logs out. The nickname is a combination of a host code unique within the network and the sequence ID specific to host and guaranteed to be unique on the host. Both codes are alphanumeric to provide maximum flexibility within nine characters. The chat proxy 39 then rewrites the IRC command with the nine character nickname and sends
25 it to the IRC server 40 (reference 41). On the other hand, the IRC server 40 sends (reference 44) data to the client 20 (which is the reverse procedure of the incoming proxy), wherein the chat proxy (converting means) 39 effects the reverse translation. The chat proxy 39 can cache the translation to prevent performance problems with constant look-up in a storage device (cache) 42.

[0080] According to the present invention semi-private chat rooms (with an additional access control) can be provided. Therefore, a menu-driven interface is provided to add access control to private and semi-private chats. An access control data base 43 which is not part of the IRC server 40 is provided within a server 1: When a chat client 20 issues requests to join a chat in the standard IRC manner, an access control is first performed by the chat proxy 39 by accessing the ACL (access control data base) 43, and then upon successful access the name translation as stated above is performed.

35 [0081] Furthermore supplemental chat room attributes can be provided.

[0082] When a user creates a chat, the user is first authenticated whether he is an authorized member. Then the user is prompted to supply attributes that will further define the chat to be created, as for example description, categories (interest groups) and the type of chat (on-going, periodic, temporary, fixed one-time). These attributes are available from the chat proxy 39 by issuing a command, which allows the chat client the access to the directory service's data
40 base without having to use a direct access protocol. The attributes of the chat may be changed using another command to the chat proxy 39 as well as via a direct access to the DS (directory services 27) data base.

[0083] With reference to Fig. 6 it will now be explained how a user can build up a communication with the IRC server 40.

[0084] In a step S1 the client issues a command to initiate a chat through the chat proxy 39. The chat proxy 39 requests the session name of the session manager (step S2). The session manager returns the name (step S3). This name is limited to nine characters corresponding to the IRC protocol. In a step S4 the chat proxy 39, which represents the converting means, rewrites the IRC command with a new name. In a step S5 the chat proxy 39 establishes the chat with the IRC server 40. Then the IRC server 40 can respond to the client (step S6), and the user can communicate (step S7). Then it is checked whether the user exists in a step S9. In case the user does not exist, the chat proxy 39 rewrites the command (step S8) and the IRC server 40 again responds to the client. In case it is decided in step S9 that the user
50 exists, the procedure is completed (step S10).

Claims

- 55 1. Communication method for a network comprising at least one server (1) and a plurality of user terminals (3), wherein the user terminals (3) can communicate with each other by means of an IRC server (40), comprising the following steps

the converting means (39) comprises a storage means (42) for caching the conversion of a sender address once the session manager (23) had been contacted for the conversion of a sender address.

11. Communication network according to anyone of the claims 7 to 10,
5 characterized in that

an access control database (43) is connected to the converting means (39) to effect an access control for the
access to the IRC server (40) by checking access information stored in an access control database (43).

10

15

20

25

30

35

40

45

50

55

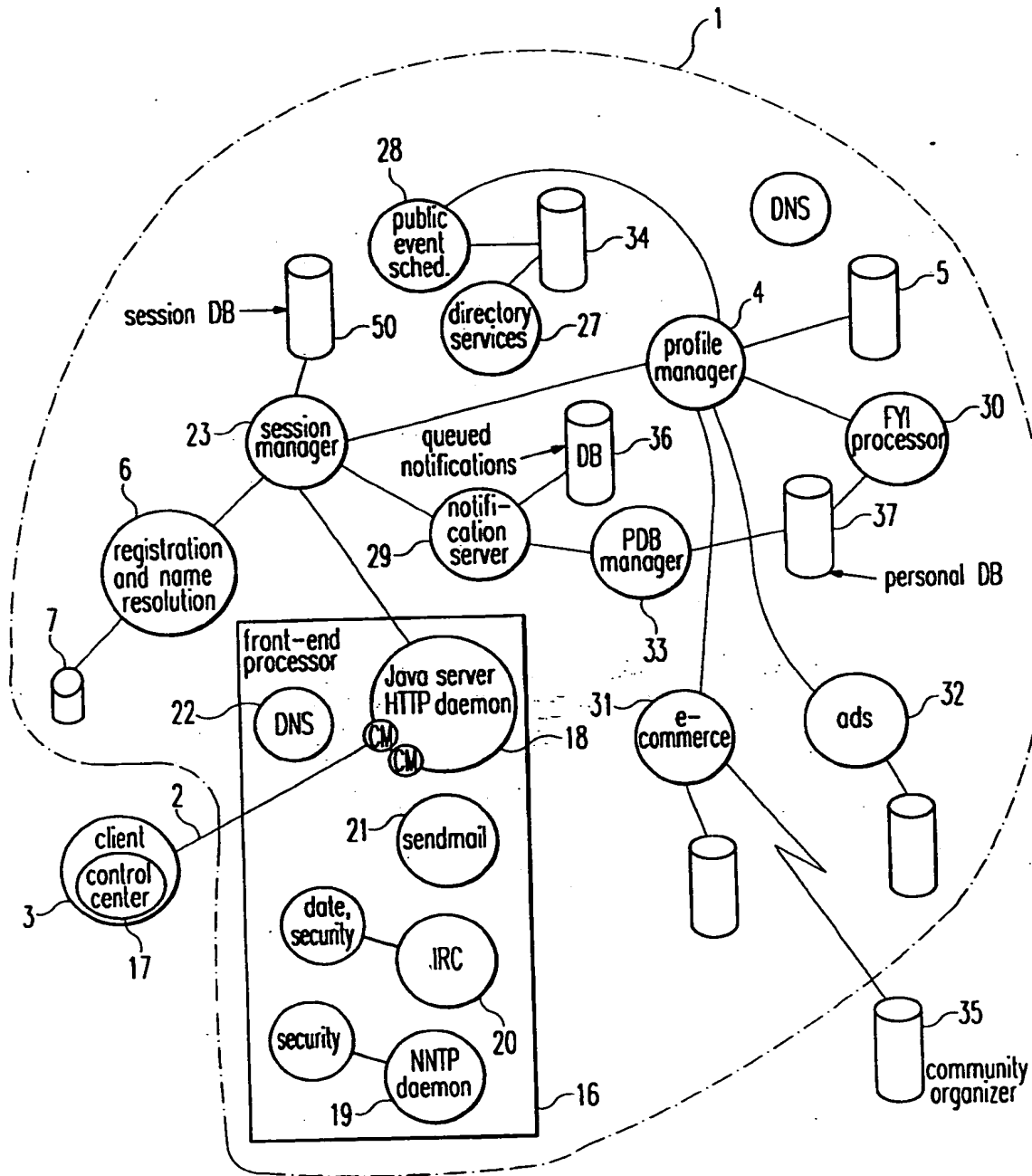


Fig. 2

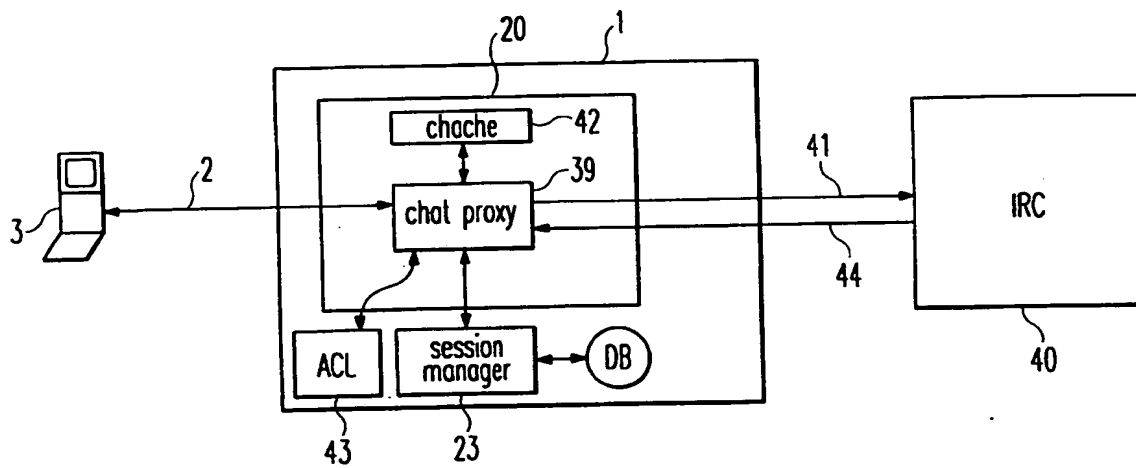


Fig. 5



European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 98 10 4934

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
A	J. OIKARINEN & D. REED: "Internet Relay Chat Protocol - RFC 1459" NETWORK WORKING GROUP, May 1993, pages 1-66, XP002076695 http://www.1rchelp.org/1rchelp/rfc1459.htm 1 * page 5, line 1, paragraph 1 - page 7, paragraph 2 * * page 20, paragraph 4.2.3 - page 24, paragraph 4.2.6 *	1-11	G06F17/00 H04L29/12
A	US 5 307 494 A (YASUMATSU KAZUKI ET AL) 26 April 1994 * abstract; claim 1 *	1,2,7,8	
A	US 5 245 656 A (LOEB SHOSHANA K ET AL) 14 September 1993 * abstract *	1,2,7,8	
A	GALL U ET AL: "Promondia: a Java-based framework for real-time group communication in the Web" COMPUTER NETWORKS AND ISDN SYSTEMS, vol. 29, no. 8-13, September 1997, page 917-926 XP004095291		TECHNICAL FIELDS SEARCHED (Int.Cl.6) H04L
The present search report has been drawn up for all claims			
Place of search THE HAGUE		Date of completion of the search 9 September 1998	Examiner Fournier, C
CATEGORY OF CITED DOCUMENTS X: particularly relevant if taken alone Y: particularly relevant if combined with another document of the same category A: technological background O: non-written disclosure P: intermediate document		T: theory or principle underlying the invention E: earlier patent document, but published on, or after the filing date D: document cited in the application L: document cited for other reasons S: member of the same patent family, corresponding document	